Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/KR04/003212

International filing date: 08 December 2004 (08.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: KR
Number: 10-2004-0050346
Filing date: 30 June 2004 (30.06.2004)

Date of receipt at the International Bureau: 02 February 2005 (02.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2004년 제 0050346 호
Application Number 10-2004-0050346

출 원 년 월 일 : 2004년 06월 30일
Date of Application JUN 30, 2004

출 원 인 : 한국전자통신연구원 외 5명
Applicant(s) Electronics and Telecommunications Research Institute, et al.

2004 년 12 월 27 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2004.06.30

【발명의 명칭】 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청과 생성 및 분배 방법 및 그 장치와, 그 프로토콜 구성 방법

【발명의 영문명칭】 METHOD FOR REQUESTING, GENERATING AND DISTRIBUTING TRAFFIC ENCRYPTION KEY ACCORDING TO SERVICES IN WIRELESS PORTABLE INTERNET SYSTEM AND APPARATUS THEREOF, AND PROTOCOL CONFIGURATION METHOD IN THE SAME

【출원인】

【명칭】 한국전자통신연구원

【출원인코드】 3-1998-007763-8

【출원인】

【명칭】 삼성전자 주식회사

【출원인코드】 1-1998-104271-3

【출원인】

【명칭】 주식회사 케이티

【출원인코드】 2-1998-005456-3

【출원인】

【명칭】 주식회사 케이티프리텔

【출원인코드】 1-1998-098986-8

【출원인】

【명칭】 에스케이텔레콤 주식회사

【출원인코드】 1-1998-004296-6

【출원인】

【명칭】 하나로통신 주식회사

【출원인코드】 1-1998-112749-2

【대리인】

【명칭】 유미특허법인

【대리인코드】 9-2001-100003-6

【지정된변리사】 이원일

【포괄위임등록번호】 2001-038431-4
【포괄위임등록번호】 2002-036528-9
【포괄위임등록번호】 2003-082444-7
【포괄위임등록번호】 2002-031524-6
【포괄위임등록번호】 2002-062290-2
【포괄위임등록번호】 2004-014783-3
【발명자】
【성명의 국문표기】 조석헌
【성명의 영문표기】 CHO,SEOK HEON
【주민등록번호】 770127-1543416
【우편번호】 570-976
【주소】 전라북도 익산시 신동 775-21번지
【국적】 KR
【발명자】
【성명의 국문표기】 박애순
【성명의 영문표기】 PARK,AE SOON
【주민등록번호】 640920-2401130
【우편번호】 305-755
【주소】 대전광역시 유성구 어은동 한빛아파트 138동 301호
【국적】 KR
【발명자】
【성명의 국문표기】 윤철식
【성명의 영문표기】 YOON,CHUL SIK
【주민등록번호】 641220-1009115
【우편번호】 139-231
【주소】 서울특별시 노원구 하계동 255-1번지 선경아파트 4동 402호
【국적】 KR
【발명자】
【성명의 국문표기】 김경수
【성명의 영문표기】 KIM,KYUNG SOO
【주민등록번호】 570129-1403316

【우편번호】 305-707

【주소】 대전광역시 유성구 신성동 한울아파트 109동 1702호

【국적】 KR

【발명자】

【성명의 국문표기】 안지환

【성명의 영문표기】 AHN,JEE HWAN

【주민등록번호】 560617-1460611

【우편번호】 305-804

【주소】 대전광역시 유성구 신성동 149-7번지

【국적】 KR

【우선권주장】

【출원국명】 KR

【출원종류】 특허

【출원번호】 10-2003-0088895

【출원일자】 2003.12.09

【증명서류】 첨부

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
유미특허법인 (인)

【수수료】

【기본출원료】	0	면	38,000 원
【가산출원료】	35	면	0 원
【우선권주장료】	1	건	20,000 원
【심사청구료】	22	항	813,000 원
【합계】	871,000 원		

【첨부서류】 1. 우선권증명서류 원문[특허청기제출]_1통

【요약서】

【요약】

본 발명은 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청과 생성 및 분배 방법 및 그 장치와, 그 프로토콜 구성 방법에 관한 것이다. 가입자 단말은 서비스별로 트래픽 암호화 키를 요청하는 키 요청 메시지를 MAC 메시지를 이용하여 기지국으로 송신한다. 기지국은 가입자 단말로부터 송신된 키 요청 메시지를 분석하여 요청된 서비스별 트래픽 암호화 키를 생성한다. 그 후, 기지국은 생성된 서비스별 트래픽 암호화 키를 포함하는 키 응답 메시지를 MAC 메시지를 이용하여 가입자 단말로 송신한다. 이 때, 기지국에서 키 생성이 실패하는 경우, 기지국은 키 생성 실패 이유를 포함하는 키 거절 메시지를 생성하여 가입자 단말로 송신한다. 본 발명에 따르면, 시스템에서 제공하는 다양한 서비스별 트래픽 암호화 키를 할당할 수 있는 기능이 지원가능하게 되고, 그 결과 멀티캐스트 서비스나 브로드캐스트 서비스와 같은 다양한 서비스를 안정적으로 제공할 수 있기 때문에 많은 가입자를 유도해 서비스의 활성화를 도모할 수 있다.

【대표도】

도 5

【색인어】

무선 휴대 인터넷, 트래픽 암호화 키, MAC 메시지, PKM, privacy, IEEE 802.16

【명세서】

【발명의 명칭】

무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청과 생성 및 분배 방법 및 그 장치와, 그 프로토콜 구성 방법 {METHOD FOR REQUESTING, GENERATING AND DISTRIBUTING TRAFFIC ENCRYPTION KEY ACCORDING TO SERVICES IN WIRELESS PORTABLE INTERNET SYSTEM AND APPARATUS THEREOF, AND PROTOCOL CONFIGURATION METHOD IN THE SAME}

【도면의 간단한 설명】

도 1은 무선 휴대 인터넷의 개요를 도시한 개략도이다.

도 2는 무선 휴대 인터넷 시스템의 계층 구조를 도시한 계층도이다.

도 3은 무선 휴대 인터넷 시스템에서 기지국과 가입자 단말의 연결구조를 도시한 개략도이다.

도 4는 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서 가입자 단말의 초기 접속 흐름도이다.

도 5는 도 4에 도시된 서비스별 트래픽 암호화 키 생성 및 분배 과정의 상세 흐름도이다.

도 6은 도 5에 도시된 서비스별 트래픽 암호화 키 생성 및 분배 과정에서 키 요청 메시지에 포함되는 파라미터 테이블을 도시한 도면이다.

도 7은 도 6에 도시된 서비스 타입 파라미터의 속성을 나타내는 도면이다.

도 8은 도 6에 도시된 멀티캐스트 서비스 그룹 아이디 필드의 속성을 나타내는 도면이다.

도 9는 도 5에 도시된 서비스별 트래픽 암호화 키 생성 및 분배 과정에서 키 거절 메시지에 포함되는 에러 코드를 나타내는 테이블을 도시한 도면이다.

도 10은 본 발명의 실시예에 따른 서비스별 트래픽 암호화 키 생성 및 분배 장치의 블록도이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<11> 본 발명은 무선 휴대 인터넷 시스템에서의 보안에 관한 것으로, 보다 구체적으로 무선 휴대 인터넷 시스템에서 서비스별로 트래픽 암호화 키를 생성 및 분배하는 장치 및 그 방법과, 그 프로토콜 구성 방법에 관한 것이다.

<12> 무선 휴대 인터넷은 종래의 무선 LAN과 같이 고정된 액세스 포인트(Access Point:AP)를 이용하는 근거리 데이터 통신 방식에 이동성(mobility)을 더 지원하는 차세대 통신 방식이다.

<13> 이러한 무선 휴대 인터넷은 다양한 표준들이 제안되고 있으며, 현재 IEEE 802.16을 중심으로 휴대 인터넷의 국제 표준화가 진행되고 있다.

<14> 도 1은 무선 휴대 인터넷의 개요를 도시한 개략도이다.

<15> 도 1에 도시된 바와 같이, 무선 휴대 인터넷 시스템은 기본적으로 가입자 단말기(10), 가입자 단말기(10)와 무선 통신을 수행하는 기지국(20, 21), 기지국(20, 21)과 게이트웨이를 통해 접속된 라우터(30, 31)를 포함한다.

<16> 종래의 IEEE 802.11과 같은 무선 LAN 방식은 고정된 액세스 포인트를 중심으로 근거리내에서 무선 통신이 가능한 데이터 통신 방식을 제공하고 있으나, 이는 가입자 단말기(Subscriber Station; 이하 "SS"라고 함)의 이동성을 제공하는 것이 아니고, 단지 유선이 아닌 무선으로 근거리 데이터 통신을 지원한다는 한계를 가지고 있었다.

<17> 한편, IEEE 802.16 그룹 등에서 추진중인 무선 휴대 인터넷 시스템은 도 1에 도시된 가입자 단말(10)이 기지국(20)이 관장하는 셀에서 기지국(21)이 관장하는 셀로 이동하는 경우에도 그 이동성을 보장하여 끊기지 않는 데이터 통신 서비스를 제공하게 된다.

<18> 이러한 IEEE 802.16은 기본적으로 도시권 통신망(Metropolitan Area Network, MAN)을 지원하는 규격으로서, 구내 정보 통신망(LAN)과 광역 통신망(WAN)의 중간 정도의 지역을 망라하는 정보 통신망을 의미한다.

<19> 따라서, 무선 휴대 인터넷 시스템은 이동통신 서비스와 같이 가입자 단말(10)의 핸드오버를 지원하며, 가입자 단말의 이동에 따라 동적인 IP 어드레스 할당을 수행하게 된다.

<20> 여기서, 무선 휴대 인터넷 가입자 단말(10)과 기지국(20, 21)은 직교 주파수 분할 다중화(Orthogonal Frequency Division Multiple Access; 이하 OFDMA라고 함)방식으로 통신을 수행한다. OFDMA 방식은 복수의 직교주파수의 부반송파(sub carrier)를

복수의 서브 채널로 이용하는 주파수 분할 방식과, 시분할 방식(TDM) 방식을 결합한 다중화 방식이다. 이러한 OFDMA 방식은 본질적으로 다중 경로(multi path)에서 발생하는 페이딩(fading)에 강하며, 데이터 전송률이 높다.

<21> 도 2는 무선 휴대 인터넷 시스템의 계층 구조를 도시한 계층도이다.

<22> 도 2에 도시된 바와 같이, IEEE 802.16의 무선 휴대 인터넷 시스템의 계층 구조는 크게 물리 계층(Physical Layer, L10)과 매체 접근 제어(Media Access Control; 이하 "MAC" 이라고 함) 계층(L21, L22, L23)으로 구분된다.

<23> 물리 계층(L10)은 변복조 및 코딩 등 통상의 물리 계층에서 수행하는 무선 통신 기능을 담당하고 있다.

<24> 한편, 무선 휴대 인터넷 시스템은 유선 인터넷 시스템과 같이 그 기능별로 세분화된 계층을 가지지 않고 하나의 MAC 계층에서 다양한 기능을 담당하게 된다.

<25> 그 기능별로 서브 계층을 살펴보면, MAC 계층은 프라이버시 서브계층(Privacy Sublayer, L21), MAC 공통부 서브계층(MAC Common Part Sublayer, L22), 서비스 특정 집합 서브계층(Service Specific Convergence Sublayer, L23)을 포함한다.

<26> 프라이버시 서브계층(L21)은 장치 인증 및 보안키 교환, 암호화 기능을 수행한다. 프라이버시 서브계층(L21)에서 장치에 대한 인증만이 수행되고, 사용자 인증은 MAC의 상위 계층(도시 생략)에서 수행된다.

<27> MAC 공통부 서브계층(L22)은 MAC 계층의 핵심적인 부분으로서 시스템 액세스, 대역폭 할당, 트래픽 연결(Traffic Connection) 설정 및 유지, QoS 관리에 관한 기능을 담당한다.

<28> 서비스 특정 집합 서브계층(L23)은 연속적인 데이터 통신에 있어서, 페이로드 헤더 서프레션(suppression) 및 QoS 맵핑 기능을 담당한다.

<29> 도 3은 무선 휴대 인터넷 시스템에서 기지국(Base Station, 이하 "BS"라고 함)과 가입자 단말의 연결구조를 도시한 개략도이다.

<30> 도 3에 도시된 바와 같이, 가입자 단말(SS)의 MAC 계층과 기지국(BS)의 MAC 계층은 트래픽 연결(Traffic Connection, C1)이라는 개념이 존재한다.

<31> 여기서, "트래픽 연결(C1)"이란 용어는 물리적 연결관계가 아니라 논리적 연결관계를 의미하는 것으로서, 하나의 서비스 플로우에 대하여 트래픽을 전송하기 위해 가입자 단말(SS)과 기지국(BS)의 MAC 동위계층(peer)들 사이의 맵핑 관계로 정의된다.

<32> 따라서, 상기 트래픽 연결(C1) 상에서 정의되는 파라미터 또는 메시지는 MAC 동위 계층간의 기능을 정의한 것이며, 실제로는 그 파라미터 또는 메시지가 가공되어 프레임화되어 물리 계층을 거쳐 전송되고, 상기 프레임을 분석하여 MAC 계층에서 그 파라미터 또는 메시지에 대응하는 기능을 수행하게 되는 것이다.

<33> 그 밖에도 MAC 메시지는 각종 동작에 대한 요청(REQ), 응답(RSP), 확인(ACK)기능을 수행하는 다양한 메시지를 포함한다.

<34> 한편, IEEE 802.16 무선 휴대 인터넷 시스템에서는 안정성 있는 서비스를 제공하기 위해 트래픽 데이터에 대한 암호화 기능을 정의하고 있다. 트래픽 데이터에 대한 암호화 기능은 서비스의 안정성 및 망의 안정성을 위해 필요한 요구사항으로 대두되고 있고, 정당한 서비스를 제공하기 위한 기본 조건이다.

<35> 종래 IEEE 802.16 무선 휴대 인터넷 시스템에서는 트래픽 데이터를 암호화하기 위해 트래픽 연결 설정 절차에 앞서서 해당 트래픽 연결에 사용될 트래픽 암호화 키를 생성하고 분배하는 방식을 정의하고 있다. 구체적으로, 가입자 단말과 기지국은 트래픽 암호화 키의 생성 및 분배를 위해, 인증 관련 메시지인 PKM-REQ(Privacy Key Managment - Request) 메시지와 PKM-RSP(Privacy Key Managment - Response) 메시지를 사용한다. 즉, 단말은 PKM-REQ 메시지 중 하나의 내부 메시지인 키 요청(Key Request) 메시지를 기지국으로 전송함으로써 트래픽 암호화 키 할당을 요구하고, 기지국은 이에 대한 응답을 단말로 보낸다. 구체적으로, 기지국은 트래픽 암호화 키 할당이 성공하였을 경우에는 키 응답(Key Reply) 메시지를 단말로 송부하고, 실패하였을 경우에는 키 거절(Key Reject) 메시지를 단말로 전송한다. 이와 같은 트래픽 암호화 키 할당 절차를 통해 할당받은 트래픽 암호화 키를 이용하여 단말과 기지국은 모든 트래픽 데이터를 암호화하여 전송한다.

<36> 이와 같은 기존의 IEEE 802.16 무선 휴대 인터넷 시스템에서 정의하는 트래픽 암호화 키 생성 및 분배 방식은 단말과 기지국 사이의 유니 캐스트(unicast) 서비스에만 국한되어 있다.

<37> IEEE 802.16 무선 휴대 인터넷 시스템이 더욱 더 많은 가입자에게 확장성 있는 서비스를 제공하고 다양한 서비스를 안정적으로 제공하기 위해서는 유니캐스트 서비스뿐만 아니라 멀티캐스트(Multicast) 서비스와 브로드캐스트(Broadcast) 서비스까지도 고려해야 할 필요가 있다.

<38> 그러나, IEEE 802.16 무선 휴대 인터넷 시스템에서 멀티캐스트 서비스나 브로드캐스트 서비스를 제공할 경우 서비스 암호화를 위하여 고려하여야 할 사항들이 존재

한다. 즉, 해당 멀티 캐스트 서비스에 가입하지 않은 동일 시스템의 사용자들에 대한 서비스를 제한하거나, 브로드 캐스트 서비스를 제공할 경우 타 사업자의 가입자들에 대한 서비스를 제한하는 방안이 고려되어야 하는데, 이와 같은 서비스의 제한은 현재의 규격으로는 구체적인 정의가 되어 있지 않다는 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

<39> 따라서, 본 발명의 기술적 과제는 상기한 문제점을 해결하고자 하는 것으로, 무선 휴대 인터넷 시스템에서 다양한 서비스별 트래픽의 암호화를 위한 키를 생성하고 분배하는 장치 및 그 방법과, 그 프로토콜을 구성하는 방법을 제공하는 것이다.

<40> 또한, 본 발명은 서비스별 트래픽 암호화 키 생성 절차에 있어서 실패가 발생하였을 경우 수용할 수 있는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 장치 및 그 방법과, 그 프로토콜을 구성하는 방법을 제공하는 것이다.

【발명의 구성 및 작용】

<41> 상기 과제를 달성하기 위한 본 발명의 하나의 특징에 따른 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청 방법은,

<42> 무선 휴대 인터넷 시스템에서 기지국에 무선 연결된 가입자 단말이 기지국으로 서비스별 트래픽 암호화 키를 요청하는 방법으로서,

<43> a) 상기 기지국과의 트래픽 연결 설정 전에 상기 트래픽 연결에 사용될 트래픽 암호화 키를 분배받을 서비스 종류를 결정하는 단계; b) 상기 결정된 서비스 종류에 따른 트래픽 암호화 키를 요청하는 키 요청 메시지를 생성하는 단계; 및 c) 상기 생

성된 키 요청 메시지를 MAC(Media Access Control) 메시지를 이용하여 상기 기지국으로 송신하는 단계를 포함한다.

<44> 본 발명의 다른 특징에 따른 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 방법은,

<45> 무선 휴대 인터넷 시스템에서 기지국이 무선 연결된 가입자 단말에게 서비스별로 트래픽 암호화 키를 생성하여 분배하는 방법으로서,

<46> a) 상기 가입자 단말로부터 서비스별 트래픽 암호화 키를 요청하는 키 요청 메시지를 수신하는 단계; b) 상기 키 요청 메시지를 분석하여 서비스 종류를 결정하는 단계; c) 상기 결정된 서비스 종류에 따른 트래픽 암호화 키를 생성하는 단계; 및 d) 상기 생성된 트래픽 암호화 키를 포함하는 키 응답 메시지를 생성하여 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 단계를 포함한다.

<47> 본 발명의 또 다른 특징에 따른 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 프로토콜 구성 방법은,

<48> 무선 휴대 인터넷 시스템에서 기지국과 가입자 단말간에 트래픽 연결에 사용될 트래픽 암호화 키를 서비스별로 생성하여 분배하기 위한 프로토콜을 구성하는 방법으로서,

<49> a) 상기 가입자 단말이 서비스별로 트래픽 암호화 키를 요청하는 키 요청 메시지를 MAC 메시지를 이용하여 상기 기지국으로 송신하는 단계; 및 b) 상기 기지국이 상기 가입자 단말로부터 송신된 키 요청 메시지를 분석하여 상기 요청된 서비스

별 트래픽 암호화 키를 생성한 후, 상기 생성된 서비스별 트래픽 암호화 키를 포함하는 키 응답 메시지를 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 단계를 포함한다.

<50> 본 발명의 또 다른 특징에 따른 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청 장치는,

<51> 무선 휴대 인터넷 시스템에서 기지국에 무선 연결되어 상기 기지국으로 서비스별 트래픽 암호화 키를 요청하는 장치로서,

<52> 상기 기지국에게 서비스별 트래픽 암호화 키 할당을 요청하는 키 요청 메시지를 생성하는 키 요청 메시지 생성부; 상기 키 요청 메시지 생성부에서 생성된 키 요청 메시지를 MAC 메시지를 이용하여 상기 기지국으로 송신하는 키 요청 메시지 송신부; 상기 기지국으로부터 MAC 메시지를 이용하여 송신되는 키 응답 메시지 또는 키 거절 메시지를 수신하는 키 응답/거절 메시지 수신부; 상기 키 응답/거절 메시지 수신부에 의해 수신된 키 응답 메시지나 키 거절 메시지를 분석하고, 키 응답 메시지인 경우에는 트래픽 암호화 키를 추출하고, 키 거절 메시지인 경우에는 에러 종류를 분석하는 메시지 분석부; 및 상기 키요청 메시지 생성부, 키 요청 메시지 송신부, 키 응답/거절 메시지 수신부 및 메시지 분석부의 동작을 제어하여, 상기 기지국에게 서비스별 트래픽 암호화 키 할당을 요청하고, 상기 기지국으로부터 상기 요청된 키 할당에 따라 송신되는 트래픽 암호화 키 또는 에러 발생시의 에러 코드를 받아서 처리하는 키 요청 제어부를 포함한다.

<53> 본 발명의 또 다른 특징에 따른 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 장치는,

<54> 무선 휴대 인터넷 시스템에서 가입자 단말에게 서비스별로 트래픽 암호화 키를 생성하여 분배하는 장치로서,

<55> 상기 가입자 단말로부터 MAC 메시지를 이용하여 송신되는 키 요청 메시지를 수신하는 키 요청 메시지 수신부; 상기 키 요청 메시지 수신부에 의해 수신된 키 요청 메시지를 분석하고, 키 요청 메시지에 포함된 서비스 종류를 포함한 정보를 분석하는 메시지 분석부; 상기 키 요청 메시지에 의해 요청된 서비스에 대해 트래픽 암호화 키를 할당할 수 있는 지의 여부를 판단하는 가입자 식별부; 상기 메시지 분석부에 의해 분석된 서비스별 트래픽 암호화 키를 생성하는 트래픽 암호화 키 생성부; 상기 트래픽 암호화 키 생성부에서 상기 가입자 단말에 의해 요청된 서비스 종류에 따라 생성된 트래픽 암호화 키를 포함하는 키 응답 메시지를 생성하여 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 키 응답 메시지 송신부; 및 상기 키 요청 메시지 수신부, 메시지 분석부, 가입자 식별부, 트래픽 암호화 키 생성부 및 키 응답 메시지 송신부의 동작을 제어하여, 상기 가입자 단말로부터의 서비스별 트래픽 암호화 키 할당 요청에 따라 대응되는 서비스별 트래픽 암호화 키를 생성하여 분배하는 키 생성 및 분배 제어부를 포함한다.

<56> 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였다. 명세서 전체를 통하여 유사한 부분에 대해서는 동일한 도면 부호를 붙였다.

<57> 이하, 첨부된 도면을 참조하여 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 장치에 대해서 상세하게 설명한다.

<58> 도 4는 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 연결 설정을 위한 흐름도이다.

<59> 도 4를 참조하면, 가입자 단말이 기지국에 진입하면(S10), 우선 기지국은 가입자 단말과 하향링크 동기를 설정한다(S20).

<60> 이와 같이, 기지국에서 하향링크 동기가 설정되면, 가입자 단말은 상향링크 파라미터를 획득하게 된다(S30). 예를 들어, 상기 파라미터는 물리 계층의 특성(예를 들어, 신호대 잡음비)에 따른 채널 디스크립터 메시지를 포함할 수 있다.

<61> 그 후, 가입자 단말과 기지국이 레인징(Ranging) 절차를 수행한다(S40). 여기서 레인징은 가입자 단말과 기지국 간의 타이밍, 전력, 주파수 정보를 정정하여 일치시키는 것으로서, 최초에 초기 레인징(initial ranging)을 수행하고, 이후 주기적으로 주기적 레인징(periodic ranging)을 수행하게 된다.

<62> 이러한 레인징 절차(S40)가 완료되면, 가입자 단말과 기지국 간의 연결 설정을 위한 단말 기본 기능에 관한 협상이 수행된다(S50). 이러한 기본 기능에 대한 협상이 완료되면, 기지국의 가입자 단말의 인증서(Certificate)를 이용하여 가입자 단말 인증이 수행된다(S60).

<63> 가입자 단말의 인증이 완료되어 무선 휴대 인터넷의 사용 권한이 확인되면, 기지국은 가입자 단말의 장치 어드레스를 등록한다(S70). 그 후, 기지국은 DHCP 서버

또는 MIP 서버를 통해 IP 주소를 가입자 단말에 제공하여 IP 연결 설정을 수행한다 (S80).

<64> IP 주소를 부여받은 가입자 단말에게 본격적인 트래픽 서비스를 제공하기 위해서 기지국은 서비스별 트래픽 암호화 키를 생성 및 분배하는 절차를 수행한 후(S90), 각각에 대한 트래픽 연결 설정을 수행한다(S100).

<65> 도 5는 도 4에 도시된 서비스별 트래픽 암호화 키 생성 및 분배 과정의 상세 흐름도이다.

<66> 도 5를 참조하면, 가입자 단말(SS)과 기지국(BS) 간에 가입자 단말의 IP 연결 설정 절차(S10 ~ S80)가 끝나면, 가입자 단말(SS)은 본격적으로 트래픽 서비스를 제공받을 수 있게 되며, 이와 같이 제공받는 트래픽 데이터에 대한 암호화를 하기 위해 서비스별 트래픽 암호화 키 생성 및 분배 절차(S90)를 거치게 된다.

<67> 먼저, 가입자 단말(SS)은 자신이 원하는 서비스 종류에 대한 트래픽 암호화 키를 할당받기 위해 기지국(BS)으로 PKM-REQ 메시지인 키 요청(Key Request) 메시지를 송신한다(S91). 이 때, 키 요청 메시지에는 트래픽 암호화 키를 서비스별로 분배받기 위한 파라미터가 함께 전달되며, 이러한 파라미터에 대해서는 추후 설명한다.

<68> 가입자 단말(SS)에서 송신된 키 요청 메시지를 수신한 기지국(BS)은 수신된 메시지의 모든 필드 값들을 바탕으로 하여 트래픽 암호화 키 생성 메커니즘으로 해당 가입자 단말(SS)에 할당할 암호화 키를 생성한 후 그 결과를 가입자 단말(SS)로 전송하다(S93).

<69> 구체적으로, 기지국(BS)에서 가입자 단말(SS)에게 할당할 트래픽 암호화 키 생성이 성공하면, 기지국(BS)은 PKM-RSP 메시지인 키 응답(Key Reply) 메시지를 가입자 단말로 전송한다. 그러나, 만약 기지국(BS)에서 가입자 단말(SS)에게 할당할 트래픽 암호화 키 생성이 실패하면, 키 거절(Key Reject) 메시지를 가입자 단말(SS)로 전송한다. 이 때, 키 거절 메시지에는 키 할당 실패에 관련된 에러 코드가 포함되며, 이러한 에러 코드에 대해서는 추후 설명한다.

<70> 이와 같이, 기지국(BS)이 키 응답 또는 키 거절 메시지를 가입자 단말(SS)에 전송함으로써, 가입자 단말(SS)에 대한 트래픽 암호화 키 생성 및 분배 절차(S90)가 끝나게 된다.

<71> 이때, 기지국(BS)이 가입자 단말(SS)로 전송하는 키 응답 메시지에는 가입자 단말(SS)이 요구하는 서비스 종류에 따른 트래픽 암호화 키가 포함되어 있으며, 이를 수신한 가입자 단말(SS)은 해당 서비스를 제공받을 때 기지국(BS)으로부터 수신한 트래픽 암호화 키를 이용하여 트래픽 데이터에 대하여 암호화하거나 복호화를 수행한다.

<72> 도 6은 도 5에 도시된 서비스별 트래픽 암호화 키 생성 및 분배를 위해서 새로이 추가되어야 할 키 요청 메시지에 포함되는 파라미터들을 테이블에 도시한 도면이다.

<73> 도 6을 참조하면, 가입자 단말(SS)이 기지국(BS)에게 서비스별 트래픽 암호화 키 할당을 요청하는 키 요청 메시지에 포함되는 파라미터에는 서비스 타입(Service Type)과 멀티캐스트 서비스 그룹 아이디(Multicast Service Group ID)가 포함된다.

<74> 서비스 타입은 가입자 단말(SS)이 어떠한 유형의 서비스를 제공받고자 하는지를 나타낸다. 따라서, 기지국(BS)은 이 서비스 타입의 값을 보고 해당 서비스 유형에 맞게 트래픽 암호화 키를 생성하여 할당하는 것이다.

<75> 멀티캐스트 서비스 그룹 아이디는 가입자 단말(SS)이 트래픽 암호화 키를 할당받고자 하는 서비스 유형이 멀티캐스트 서비스일 때만 존재하는 것으로서, 멀티캐스트 서비스 그룹의 식별자 역할을 한다. 이 멀티캐스트 서비스 그룹 아이디는 가입자 단말(SS)이 멀티캐스트 서비스를 제공받더라도 가입하지 않은 타 멀티캐스트 서비스 그룹의 서비스에 제한을 두기 위한 목적으로도 사용된다.

<76> 도 7은 도 6에 도시된 서비스 타입 파라미터의 속성(attribute)을 나타내는 도면이다.

<77> 도 7을 참조하면, 서비스 타입 파라미터는 이 파라미터로 할당받으려는 트래픽 암호화 키의 해당 서비스 종류를 나타낸다. 예를 들어, 서비스 타입 파라미터의 타입(Type)은 '28'이고, 길이(Length)는 1 Byte이며, 그 값은 설정된 값에 따라 서비스 종류를 나타낸다. 예를 들어, 서비스 타입 파라미터의 값이 "0"이면 유니캐스트 서비스에 해당하는 트래픽 암호화 키 할당을 요구하는 것이고, "1"이면 멀티캐스트 서비스에 해당하는 트래픽 암호화 키 할당을 요구하는 것이며, "2"이면 브로드캐스트 서비스에 해당하는 트래픽 암호화 키 할당을 요구하는 것이다. 따라서, 기지국(BS)은 가입자 단말(SS)로부터 송신되는 키 요청 메시지에 포함된 서비스 타입 파라미터의 값을 참조하여 서비스별 트래픽 암호화 키를 생성하여 가입자 단말(SS)에게 분배한다.

<78> 도 8은 도 6에 도시된 멀티캐스트 서비스 그룹 아이디 필드의 속성을 나타내는 도면이다.

<79> 도 8을 참조하면, 멀티캐스트 서비스 그룹 아이디는 IEEE 802.16 무선 휴대 인터넷 시스템에서 제공하는 멀티캐스트 서비스 그룹의 식별자이다. 예를 들어, 멀티캐스트 서비스 그룹 아이디 파라미터의 타입(Type)은 '29'이고, 길이(Length)는 1 Byte이며, 그 값은 멀티캐스트 서비스 그룹의 식별자이다.

<80> 따라서, 기지국(BS)은 가입자 단말(SS)로부터 송신되는 키 요청 메시지에 포함된 멀티캐스트 서비스 그룹 아이디 파라미터의 값을 참조하여 해당 가입자 단말(SS)에 대한 멀티캐스트 서비스별 트래픽 암호화 키 생성 여부를 결정한다.

<81> 도 9는 도 5에 도시된 서비스별 트래픽 암호화 키 생성 및 분배를 위해서 새로이 추가되어야 할 키 거절 메시지에 포함되는 에러 코드를 나타내는 테이블을 도시한 도면이다.

<82> 도 9를 참조하면, 기지국(BS)이 가입자 단말(SS)에게 서비스별 트래픽 암호화 키를 할당하기 위해 해당 키를 생성하는 과정에서 실패하여 가입자 단말(SS)에게 송신하는 키 거절 메시지에 포함되며, "지원하지 않는 서비스 타입"(Unsupported Service Type)과 "권한이 없는 멀티캐스트 서비스 그룹 아이디(Unauthorized Multicast Service Group ID)를 포함한다.

<83> "지원하지 않는 서비스 타입"은 서비스별 트래픽 암호화 키를 할당받기 위해 가입자 단말(SS)로부터 송신되는 키 요청 메시지에 포함된 서비스 타입에 표시된 서비스 종류가 기지국(BS)에 의해 지원이 불가능한 값을 갖는 경우 이러한 실패 내용을

나타내기 위해 키 거절 메시지에 포함되는 에러 코드 파라미터이다. 예를 들어, 가입자 단말(SS)에서 수신되는 키 거절 메시지의 에러 코드 필드 값이 '7'이면 "지원하지 않는 서비스 타입"으로 인한 실패를 나타내도록 한다.

<84> 한편, "권한이 없는 멀티캐스트 서비스 그룹 아이디"는 가입자 단말(SS)이 키 요청 메시지에 포함된 서비스 타입 파라미터에서 멀티캐스트 서비스 종류를 나타내고, 그 때 멀티캐스트 서비스 그룹 아이디 파라미터에 기록된 식별자가 기지국(BS)에서 트래픽 암호화 키를 할당할 수 없는 식별자인 경우에 발생되는 에러 코드이다. 예를 들어, 가입자 단말(SS)에서 수신되는 키 거절 메시지의 에러 코드 필드값이 '8'이면 "권한이 없는 멀티캐스트 서비스 그룹 아이디"로 인한 실패를 나타내도록 한다.

<85> 이하, 상기한 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서 서비스별 트래픽 암호화 키 생성 및 분배를 수행하는 장치의 일예에 대해 설명한다.

<86> 도 10은 본 발명의 실시예에 따른 서비스별 트래픽 암호화 키 생성 및 분배 장치의 블록도이다.

<87> 도 10에 도시된 바와 같이, 본 발명의 실시예에 따른 서비스별 트래픽 암호화 키 생성 및 분배 장치는 기지국(100) 및 가입자 단말(200)을 포함한다.

<88> 가입자 단말(100)은 키 요청 메시지 생성부(110), 키 요청 메시지 송신부(120), 키 응답/거절 메시지 수신부(130), 메시지 분석부(140), 메모리(150) 및 키 요청 제어부(160)를 포함한다.

<89> 키 요청 메시지 생성부(110)는 기지국(200)에게 서비스별 트래픽 암호화 키 할당을 요청하는 키 요청 메시지를 생성한다. 이 때 생성되는 키 요청 메시지는 IEEE

802.16에서의 MAC 메시지 중의 하나인 PKM-REQ 메시지로써 생성되며, 상기 도 6에 도시된 바와 같은 서비스 타입과 멀티캐스트 서비스 그룹 아이디 파라미터가 포함된다.

<90> 키 요청 메시지 송신부(120)는 키 요청 메시지 생성부(110)에서 생성된 키 요청 메시지를 MAC 메시지 중 하나인 PKM-REQ 메시지를 이용하여 안테나(170)를 통해 기지국(200)으로 송신한다.

<91> 키 응답/거절 메시지 수신부(130)는 기지국(200)으로부터 MAC 메시지 중 하나인 PKM-RSP 메시지를 이용하여 송신되는 키 응답 메시지나 키 거절 메시지를 안테나(170)를 통해 수신한다.

<92> 메시지 분석부(140)는 키 응답/거절 메시지 수신부(130)에 의해 수신된 키 응답 메시지나 키 거절 메시지를 분석하고, 키 응답 메시지인 경우에는 트래픽 암호화 키를 추출하고, 키 거절 메시지인 경우에는 에러 종류를 분석한다.

<93> 메모리(150)는 메시지 분석부(140)에 의해 분석된 결과를 저장한다. 예를 들어 추출되어 추후 트래픽 전송시 암호화에 사용되는 트래픽 암호화 키를 저정하거나 또는 키 할당 실패시 발생된 에러 코드 등을 저장한다.

<94> 키 요청 제어부(160)는 기지국(200)에게 서비스별 트래픽 암호화 키 할당을 요청하고, 기지국(200)으로부터 서비스별로 할당된 트래픽 암호화 키를 받거나 아니면 에러 발생시 그 에러 코드를 받아서 처리하기 위해, 키요청 메시지 생성부(110), 키 요청 메시지 송신부(120), 키 응답/거절 메시지 수신부(130), 메시지 분석부(140) 및 메모리(150)의 동작을 제어한다.

<95> 한편, 기지국(200)은 키 요청 메시지 수신부(210), 메시지 분석부(220), 가입자 식별부(230), 메모리(240), 트래픽 암호화 키 생성부(250) 및 키 응답/거절 메시지 송신부(260) 및 키 생성 및 분배 제어부(270)를 포함한다.

<96> 키 요청 메시지 수신부(210)는 가입자 단말(100)에서 송신되는 MAC 메시지 중 하나인 PKM-REQ 메시지를 이용한 키 요청 메시지를 안테나(280)를 통해 수신한다.

<97> 메시지 분석부(220)는 키 요청 메시지 수신부(210)에 의해 수신된 키 요청 메시지를 분석하고, 키 요청 메시지에 포함된 서비스 타입 및 멀티캐스트 서비스 그룹 아이디 등의 파라미터를 분석한다.

<98> 가입자 식별부(230)는 키 요청 메시지에 의해 요청된 서비스가 멀티캐스트 서비스인 경우, 키 요청 메시지에 포함된 멀티캐스트 서비스 그룹 아이디에 기록된 식별자에 대해 트래픽 암호화 키를 할당할 수 있는 식별자인 지의 여부를 판단한다. 만약 멀티캐스트 서비스 그룹 아이디에 기록된 식별자가 트래픽 암호화 키를 할당할 수 없는 식별자인 경우에는 "권한이 없는 멀티캐스트 서비스 그룹 아이디"임을 표시한다.

<99> 메모리(240)는 메시지 분석부(220)에 의해 분석된 결과와 가입자 식별부(230)에 의해 식별된 결과 등을 저장한다.

<100> 트래픽 암호화 키 생성부(250)는 가입자 단말로부터의 트래픽 암호화 키 요청에 대하여 수락한 경우에 한해서 서비스별 트래픽 암호화 키를 생성한다.

<101> 키 응답/거절 메시지 송신부(260)는 트래픽 암호화 키 생성부(250)에서 트래픽 암호화 키 생성이 성공적으로 완료된 경우에는 생성된 트래픽 암호화 키를 포함하는

키 응답 메시지를 생성하여 MAC 메시지 중의 하나인 PKM-RSP 메시지를 이용하여 안테나(280)를 통해 가입자 단말(100)로 송신한다. 그러나, 트래픽 암호화 키 생성부(250)에서 트래픽 암호화 키 생성이 실패하는 경우, 그 실패한 이유를 나타내는 에러 코드를 포함하는 키 거절 메시지를 생성하여 PKM-RSP 메시지를 이용하여 가입자 단말(100)로 송신한다.

<102> 키 생성 및 분배 제어부(270)는 가입자 단말(100)로부터의 서비스별 트래픽 암호화 키 할당 요청에 따라 대응되는 서비스별 트래픽 암호화 키를 생성하여 분배하고, 또한 트래픽 암호화 키 생성시 에러가 발생하는 경우 그 에러 코드를 가입자 단말(100)로 전달하기 위해, 키요청 메시지 수신부(210), 메시지 분석부(220), 가입자 식별부(230), 메모리(240), 트래픽 암호화 키 생성부(250) 및 키 응답/거절 메시지 송신부(260)의 동작을 제어한다.

<103> 이상에서 본 발명의 바람직한 실시예에 대하여 상세하게 설명하였지만 본 발명은 이에 한정되는 것은 아니며, 그 외의 다양한 변경이나 변형이 가능하다.

【발명의 효과】

<104> 본 발명에 따르면, 다음과 같은 효과가 있다.

<105> 첫째, 시스템에서 제공하는 다양한 서비스별 트래픽 암호화 키를 할당할 수 있는 기능이 지원가능하게 되고, 그 결과 멀티캐스트 서비스나 브로드캐스트 서비스와 같은 다양한 서비스를 안정적으로 제공할 수 있기 때문에 많은 가입자를 유도해 서비스의 활성화를 도모할 수 있다.

<106> 둘째, 서비스 별로 트래픽 암호화 키를 생성하고 관리함으로써 서비스의 더욱 강력한 보안을 유지할 수 있다.

<107> 셋째, 멀티캐스트 서비스의 경우 멀티캐스트 서비스 그룹별로 할당된 그룹 트래픽 암호화 키가 다르므로 그룹별로 보안유지가 가능하다.

【특허청구범위】

【청구항 1】

무선 휴대 인터넷 시스템에서 기지국에 무선 연결된 가입자 단말이 기지국으로 서비스별 트래픽 암호화 키를 요청하는 방법에 있어서,

a) 상기 기지국과의 트래픽 연결 설정 전에 상기 트래픽 연결에 사용될 트래픽 암호화 키를 분배받을 서비스 종류를 결정하는 단계;

b) 상기 결정된 서비스 종류에 따른 트래픽 암호화 키를 요청하는 키 요청 메시지를 생성하는 단계; 및

c) 상기 생성된 키 요청 메시지를 MAC(Media Access Control) 메시지를 이용하여 상기 기지국으로 송신하는 단계

를 포함하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청 방법.

【청구항 2】

제1항에 있어서,

상기 b) 단계에서, 상기 서비스 종류는 상기 키 요청 메시지에 포함된 파라미터에 기록된 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청 방법.

【청구항 3】

제1항 또는 제2항에 있어서,

상기 서비스 종류에는 유니캐스터(Unicast) 서비스, 멀티캐스트(Multicast) 서비스 및 브로드캐스트(Broadcast) 서비스가 포함되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청 방법.

【청구항 4】

제3항에 있어서,

상기 서비스 종류가 멀티캐스트 서비스인 경우, 가입자에 대한 멀티캐스트 서비스 그룹의 식별자가 기록된 아이디(ID)가 상기 키 요청 메시지의 파라미터에 포함되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청 방법.

【청구항 5】

제3항에 있어서,

상기 c) 단계에서 상기 키 요청 메시지는 IEEE 802.16 표준 프로토콜의 MAC 메시지 중의 하나인 PKM-REQ(Privacy Key Managment - Request) 메시지를 이용하여 송신되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청 방법.

【청구항 6】

무선 휴대 인터넷 시스템에서 기지국이 무선 연결된 가입자 단말에게 서비스별로 트래픽 암호화 키를 생성하여 분배하는 방법에 있어서,

a) 상기 가입자 단말로부터 서비스별 트래픽 암호화 키를 요청하는 키 요청 메시지를 수신하는 단계;

b) 상기 키 요청 메시지를 분석하여 서비스 종류를 결정하는 단계;

c) 상기 결정된 서비스 종류에 따른 트래픽 암호화 키를 생성하는 단계; 및

d) 상기 생성된 트래픽 암호화 키를 포함하는 키 응답 메시지를 생성하여 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 단계

를 포함하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 방법.

【청구항 7】

제6항에 있어서,

상기 b) 단계에서, 상기 키 요청 메시지에 상기 서비스 종류 관련 파라미터가 포함되어 있으며, 상기 기지국이 상기 파라미터를 분석하여 상기 서비스 종류를 결정하는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 방법.

【청구항 8】

제6항 또는 제7항에 있어서,

상기 c) 단계에서, 상기 결정된 서비스 종류에 따른 상기 가입자 단말에 대한 트래픽 암호화 키 생성이 실패하는 경우, 상기 실패 이유를 나타내는 에러 코드를 포함하는 키 거절 메시지를 생성하여 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 방법.

【청구항 9】

제8항에 있어서,

상기 가입자 단말이 트래픽 암호화 키를 요청한 서비스 종류에 대해 트래픽 암호화 키 생성 및 분배가 불가능한 경우, 상기 기지국이 상기 에러 코드에 "지원하지 않는 서비스 타입"(Unsupported Service Type)을 기재하여 상기 가입자 단말로 송신하는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 방법.

【청구항 10】

제8항에 있어서,

상기 서비스 종류에는 유니캐스터(Unicast) 서비스, 멀티캐스트(Multicast) 서비스 및 브로드캐스트(Broadcast) 서비스가 포함되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 방법.

【청구항 11】

제10항에 있어서,

상기 가입자 단말이 트래픽 암호화 키를 요청한 서비스 종류가 멀티캐스트 서비스이고, 상기 기지국이 상기 가입자 단말에 대한 멀티캐스트 서비스 그룹 아이디에 의해 정의된 해당 멀티캐스트 서비스가 제공 불가능한 경우, 상기 에러 코드에 "권한 없는 멀티캐스트 서비스 그룹 아이디"(Unauthorized Multicast Service Group ID)를 기재하여 상기 가입자 단말로 송신하는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 방법.

【청구항 12】

제8항에 있어서,

상기 키 응답 메시지 및 키 거절 메시지는 IEEE 802.16 표준 프로토콜의 MAC 메시지 중의 하나인 PKM-RSP(Privacy Key Managment - Response) 메시지를 이용하여 송신되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 방법.

【청구항 13】

무선 휴대 인터넷 시스템에서 기지국과 가입자 단말간에 트래픽 연결에 사용될 트래픽 암호화 키를 서비스별로 생성하여 분배하기 위한 프로토콜을 구성하는 방법에 있어서,

a) 상기 가입자 단말이 서비스별로 트래픽 암호화 키를 요청하는 키 요청 메시지를 MAC 메시지를 이용하여 상기 기지국으로 송신하는 단계; 및

b) 상기 기지국이 상기 가입자 단말로부터 송신된 키 요청 메시지를 분석하여 상기 요청된 서비스별 트래픽 암호화 키를 생성한 후, 상기 생성된 서비스별 트래픽 암호화 키를 포함하는 키 응답 메시지를 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 단계

를 포함하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 프로토콜 구성 방법.

【청구항 14】

제13항에 있어서,

상기 a) 단계에서, 상기 키 요청 메시지는 IEEE 802.16 표준 프로토콜의 MAC 메시지 중 하나인 PKM-REQ 메시지를 이용하여 송신되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 프로토콜 구성 방법.

【청구항 15】

제13항에 있어서,

상기 b) 단계에서, 상기 서비스별 트래픽 암호화 키 생성 실패시, 상기 실패 이유를 기록한 에러 코드를 포함하는 키 거절 메시지를 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 프로토콜 구성 방법.

【청구항 16】

제15항에 있어서,

상기 b) 단계에서, 상기 키 응답 메시지 및 키 거절 메시지는 IEEE 802.16 표준 프로토콜의 MAC 메시지 중 하나인 PKM-RSP 메시지를 이용하여 송신되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 프로토콜 구성 방법.

【청구항 17】

무선 휴대 인터넷 시스템에서 기지국에 무선 연결되어 상기 기지국으로 서비스별 트래픽 암호화 키를 요청하는 장치에 있어서,

상기 기지국에게 서비스별 트래픽 암호화 키 할당을 요청하는 키 요청 메시지를 생성하는 키 요청 메시지 생성부;

상기 키 요청 메시지 생성부에서 생성된 키 요청 메시지를 MAC 메시지를 이용하여 상기 기지국으로 송신하는 키 요청 메시지 송신부;

상기 기지국으로부터 MAC 메시지를 이용하여 송신되는 키 응답 메시지 또는 키 거절 메시지를 수신하는 키 응답/거절 메시지 수신부;

상기 키 응답/거절 메시지 수신부에 의해 수신된 키 응답 메시지나 키 거절 메시지를 분석하고, 키 응답 메시지인 경우에는 트래픽 암호화 키를 추출하고, 키 거절 메시지인 경우에는 에러 종류를 분석하는 메시지 분석부; 및

상기 키요청 메시지 생성부, 키 요청 메시지 송신부, 키 응답/거절 메시지 수신부 및 메시지 분석부의 동작을 제어하여, 상기 기지국에게 서비스별 트래픽 암호화 키 할당을 요청하고, 상기 기지국으로부터 상기 요청된 키 할당에 따라 송신되는 트래픽 암호화 키 또는 에러 발생시의 에러 코드를 받아서 처리하는 키 요청 제어부

를 포함하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청 장치.

【청구항 18】

제17항에 있어서,

상기 키 요청 메시지에는 서비스 종류와, 상기 서비스 종류가 멀티 캐스트 서비스인 경우의 상기 가입자 단말의 멀티캐스트 서비스 그룹 아이디가 포함되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청 장치.

【청구항 19】

제17항에 있어서,

상기 키 요청 제어부의 제어에 따라, 상기 메시지 분석부에 의해 분석된 결과인 트래픽 암호화 키 또는 에러 코드 등를 포함하는 정보를 저장하는 메모리를 더 포함하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 요청 장치.

【청구항 20】

무선 휴대 인터넷 시스템에서 가입자 단말에게 서비스별로 트래픽 암호화 키를 생성하여 분배하는 기지국 장치에 있어서,

상기 가입자 단말로부터 MAC 메시지를 이용하여 송신되는 키 요청 메시지를 수신하는 키 요청 메시지 수신부;

상기 키 요청 메시지 수신부에 의해 수신된 키 요청 메시지를 분석하고, 키 요청 메시지에 포함된 서비스 종류를 포함한 정보를 분석하는 메시지 분석부;

상기 키 요청 메시지에 의해 요청된 서비스에 대해 트래픽 암호화 키를 할당할 수 있는 지의 여부를 판단하는 가입자 식별부;

상기 메시지 분석부에 의해 분석된 서비스별 트래픽 암호화 키를 생성하는 트래픽 암호화 키 생성부;

상기 트래픽 암호화 키 생성부에서 상기 가입자 단말에 의해 요청된 서비스 종류에 따라 생성된 트래픽 암호화 키를 포함하는 키 응답 메시지를 생성하여 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 키 응답 메시지 송신부; 및

상기 키 요청 메시지 수신부, 메시지 분석부, 가입자 식별부, 트래픽 암호화 키 생성부 및 키 응답 메시지 송신부의 동작을 제어하여, 상기 가입자 단말로부터의 서

비스별 트래픽 암호화 키 할당 요청에 따라 대응되는 서비스별 트래픽 암호화 키를 생성하여 분배하는 키 생성 및 분배 제어부

를 포함하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 장치.

【청구항 21】

제20항에 있어서,

상기 키 생성 및 분배 제어부의 제어에 따라, 상기 트래픽 암호화 키 생성부에서 상기 가입자 단말에 의한 요청에 대해 에러가 발생하는 경우, 그 에러 코드를 포함하는 키 거절 메시지를 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 키 거절 메시지 송신부

를 더 포함하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 장치.

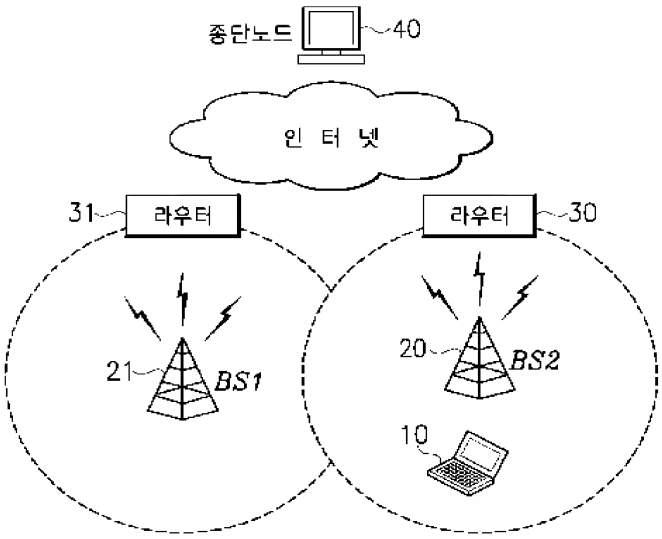
【청구항 22】

제20항에 있어서,

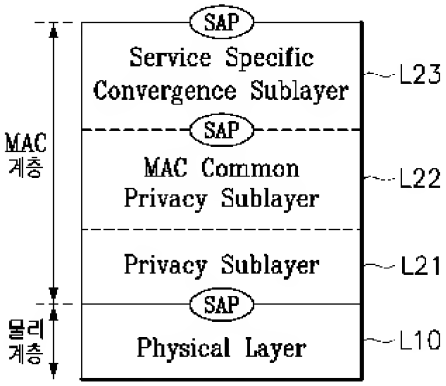
상기 키 생성 및 분배 제어부의 제어에 따라, 상기 메시지 분석부에 의해 분석된 결과 및 상기 가입자 식별부에 의해 식별된 결과를 포함하는 정보를 저장하는 메모리를 더 포함하는 무선 휴대 인터넷 시스템에서의 서비스별 트래픽 암호화 키 생성 및 분배 장치.

【도면】

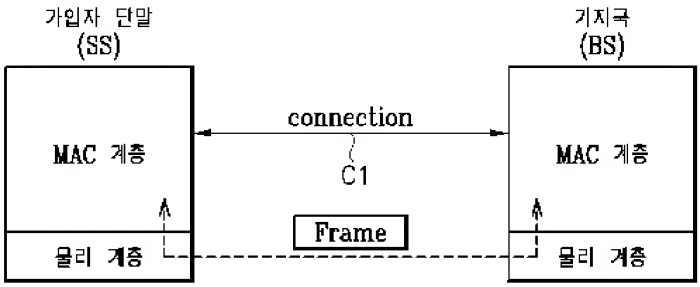
【도 1】


종단노드
40
인 터 넷
31
라우터
라우터
30
21
BS1
20
BS2
10

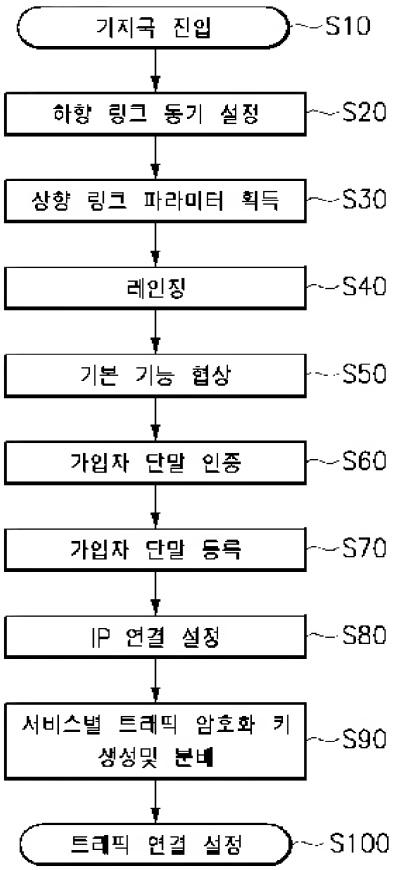
【도 2】


SAP
Service Specific Convergence Sublayer
L23
SAP
MAC Common Privacy Sublayer
L22
Privacy Sublayer
L21
SAP
Physical Layer
L10
MAC 계층
물리 계층

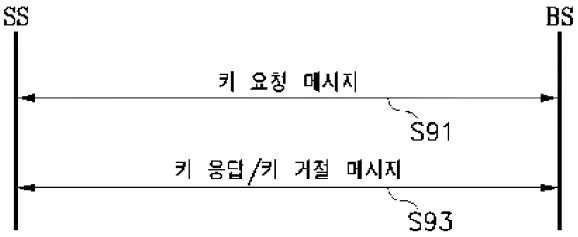
【도 3】


가입자 단말
(SS)
기지국
(BS)
MAC 계층
connection
C1
MAC 계층
Frame
물리 계층
물리 계층

【도 4】



【도 5】



【도 6】

Attribute	Contents
Service Type	Service Type (Unicast or multicast or broadcast)
Multicast Service Group ID	Identifier of multicast service group

【도 7】

Type	Length	Value
28	1	0: Unicast Service 1: Multicast Service 2: Broadcast Service 3-255: Reserved

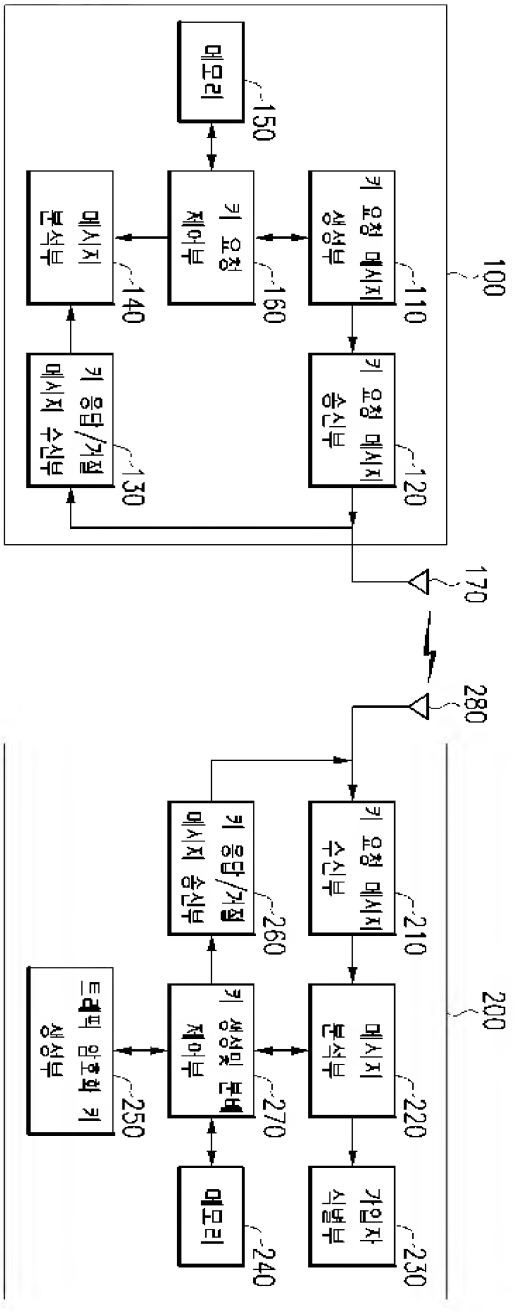
【도 8】

Type	Length	Value
29	1	Identifier of the multicast service group

【도 9】

Error Code	Messages	Contents
7	Key Reject	Unsupported Service Type
8	Key Reject	Unauthorized Multicast Service Group ID

【도 10】


100
메모리
150
키 요청 메시지 생성부
110
키 요청 제어부
160
메시지 분석부
140
키 요청 메시지 송신부
120
키 응답/거절 메시지 수신부
130
170
280
200
키 요청 메시지 수신부
210
키 응답/거절 메시지 송신부
260
메시지 분석부
220
키 생성 및 분배 제어부
270
트래픽 암호화 키 생성부
250
메모리
240
가입자 식별부
230